

5 June 1980

MEMORANDUM FOR: Members, APEX Steering Committee

STATINTL

FROM: [redacted]  
Chairman, Panel 4

SUBJECT: APEX

STAT

1. At their 3 June 1980 meeting, the APEX Steering Group discussed at some length the concerns expressed by representatives of the [redacted] and Navy related to over-exposure of some contractors in consequence of implementing APEX access approval requirements. Toward a goal of circumscribing the scope of the concerns and defining viable alternatives to current prescriptions, the Chairman of the APEX Steering Group established APEX Panel 4. I accepted the Chairmanship.

STAT

2. If you perceive difficulties similar to those expressed by the [redacted] and Navy representatives, it is requested that you designate a representative to serve on Panel 4 and have him contact me [redacted] on time to attend an early meeting. Members should come to the first meeting prepared to present their perceptions of difficulties in only that degree of specificity necessary to identify common elements of concern. Subsequently, it will be the responsibility of your member to evaluate the need for special accesses and to arrange for members of Panel 4 to be granted them for the duration of the Panel's efforts.

STATINTL

3. Attached are some thoughts and observations that may be of general assistance as Panel 4 goes about its task.

STATINTL



Attachment

NSA review  
completed



5 June 1980

APEX - Panel 4 - General Observation

1. The foundation of information security is a personnel security program that verifies the trustworthiness of employees and a physical security program to assure information is available only to trustworthy personnel.
2. The APEX Special Access Program is an administrative formalization of the need-to-know principle intended to restrict access to the minimum amount of information necessary for an essential core of personnel within the total population of trusted employees to discharge their assignments.
3. The crux of the presently addressed concern appears to rest on a lack of specificity of what constitutes the "minimum amount of information necessary" and confusion related to establishment of parameters circumscribing the "essential core of personnel."
4. There are some guides that may be of assistance in defining "minimum amount of information."
  - a. First, in order to be compartmented under APEX the information must be classifiable in accordance with the two tests mandated by E.O. 12065; i.e., (1) the information must fall within one of seven classification criteria such as intelligence sources and the design of weapons and (2) unauthorized disclosure of the information must result in at least identifiable damage. Further, the information must be marked conspicuously to put users on notice of its current classification status and to show any special distribution restrictions.
  - b. Second, the information must be National Foreign Intelligence identifiable in the words of the Presidential Directive/NSC-55 as "particularly sensitive intelligence sources and methods."

5. There are statements in the Final Report of the NFIB Working Group on Compartmentation which emphasize that care is to be exercised in selection of material for inclusion in APEX. One of the major objectives of the APEX System is given as:

"The development of a system which will carefully restrict to special access programs and systems of compartmentation only that intelligence which clearly warrants special protection..." and meant to "keep out of compartmentation information which has been overclassified and unnecessarily compartmented."

6. There are some guides which may be of assistance in identifying the "essential core of personnel." Among these are:

a. the fact that the individual requires access to classified information for the performance of official duties. This presumes that recognizable classified material is at issue and the individual knows that he is being made privy to it;

b. the fact that personnel nominated for APEX must be certified by the SIO as having a need to know for specific aspects of the system. This presumes that personnel will be selected to do something specifically and identifiably related to the activity protected under APEX;

c. the fact that personnel nominated must meet uniform personnel security criteria; and

d. the fact that as a condition of access to APEX personnel must be provided a security indoctrination telling them what it is they are to protect "and general information about the APEX system." Further, personnel are to execute a nondisclosure agreement.

7. In drafting the APEX Manual it was recognized that there would be different levels of access required by different categories of personnel. These types of access are identified as APEX General, Phase I and Phase II; and APEX (Operational), Phase I and II. Careful application of the guidance provided in the Manual for granting these types and phases of access will be of assistance in defining the "core of essential personnel" who require access.